SYNOPSIS

Ph.D in Computer Science

COMPLEXITY AWARE INTELLIGENT INTRUSION DETECTION FOR DDOS ATTACKS

By

KALAIVANI M.

(18PHCSP005)

Supervisor

Dr. G. PADMAVATHI

Department of Computer Science

Submitted to

Avinashilingam Institute for Home Science and Higher Education for Women,
Coimbatore - 641 043

JULY 2024

1. Introduction

The rise of Distributed Denial of Service (DDoS) attacks represents a significant and growing threat to the stability and security of digital infrastructures worldwide [1]. Effective detection of these attacks requires sophisticated methods to accurately identify malicious activity amidst vast amounts of network traffic. Complexity aware intelligent intrusion system with enhanced feature engineering plays a crucial role in improving the performance of intrusion detection systems (IDS). This thesis proposes an innovative methodology to enhance DDoS attack detection using Machine Learning (ML) and Deep Learning (DL) techniques with bio-inspired optimization. Traditional Intrusion Detection Systems (IDSs) often struggle with feature selection due to the complexity and volume of real-world data. To address this, the proposed methodology integrates ML and DL models to classify network traffic and set appropriate thresholds for attack detection. The methodology comprises four key steps: data collection, data preprocessing, implementation of proposed techniques, and performance evaluation. The data collection step involves utilizing benchmark datasets such as CICDDoS2019, UNSW-NB15, and NSL-KDD for comprehensive analysis. Data preprocessing involves standardization and normalization techniques to address overfitting issues and ensure efficient feature extraction.

The proposed methodology introduces complexity aware solutions for attack detection through four contributions. Phase 1 suggests Ensemble Based Combined Filter for Feature Selection (CFFS) With Decision Tree C 4.5 (DT) Classifier for Single DDoS Flooding Attacks Detection exhibiting improved detection rates and rapid execution time over existing methods. Phase 2 suggests a Feature Engineering Techniques with Hybridization of Dragonfly Optimization Algorithm (DOA) And Decision Tree C 4.5 Classification Algorithm (DT) For Multiple DDoS Flooding Attacks Detection, showcasing enhanced accuracy and less detection time in detecting multiple DDoS flood attacks. Phase 3 presents a Panthera Leo Optimized Multilayer Feed Forward Learning for Multi Vector DDoS Attack Detection, that outperforms traditional learning models in terms of improving detection accuracy and reducing computational overhead. Phase 4 proposes the Attention Enabled Gated Recurrent Network (AEGRN) and Deep Feed Forward Networks for Detecting DDoS Attacks in Multiple Datasets with low computational overhead, improved accuracy and high-speed, demonstrating superior performance compared to other algorithms.

Performance evaluation metrics including accuracy, recall, specificity, precision, and F1-score are employed across all contributions to assess the effectiveness of the proposed

methodologies. Experimental results validate the efficacy of the proposed techniques in enhancing DDoS attack detection. Overall, this research work contributes to the advancement of DDoS attack detection through innovative ML and DL approaches, offering robust solutions for safeguarding IT landscape against evolving cyber threats.

2. Literature Study

Distributed Denial of Service (DDoS) detection methods has garnered significant attention in literature. DDoS attacks are a prevalent form of cyber threat that can disrupt online services by overwhelming them with a flood of traffic from multiple sources. Detecting these attacks is crucial for maintaining the availability and integrity of online systems. Researchers have explored various approaches and techniques to identify and mitigate DDoS attacks effectively. Understanding the strengths and limitations of these detection techniques is essential for developing robust defense mechanisms against DDoS attacks in today's interconnected digital landscape. The literature is carried out on the topics: various approaches in DDoS detection, existing IDS in intrusion detection, various datasets used in intrusion detection, various feature selection (FS) methods, and various computational intelligence techniques in intrusion detection. The significant literatures are shown in Table 1.

Table 1 Significant Literature on DDOS detection

Author, Year and Journal	Title	Techniques Applied	Dataset	Findings
Aswani Devi Aguru, Suresh Babu Erukala (2024) **ELSEVIER**	A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning	Modified Gated Recurrent Units (mGRU)	CICIoT 2023, CICDDoS2019	mGRU-based IDS models outperform standard GRU-based IDS models with a 2% reduction in time consumption. Suitable for time-critical healthcare applications.
Devrim Akgun, Selman Hizal, Unal Cavusoglu, (2022) **ELSEVIER**	A new DDoS attacks intrusion detection model based on deep learning for cybersecurity	Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Long Short Term Memory (LSTM).	CIC-DDoS2019 dataset.	CNN-based inception model, achieved high accuracy rates of 99.99% for binary and 99.30% for multiclass detection on the CIC-DDoS2019 dataset.
Mohamed Aly Bouke, Azizol Abdullah, Sameer Hamoud ALshatebi, Mohd Taufik Abdullah, Hayate El Atigh, (2023) **Microprocessors and Microsystems**	An intelligent DDoS attack detection tree-based model using Gini index feature selection method	Decision Tree (DT) algorithm, enhanced Gini index feature selection method.	UNSW-NB15 dataset	The proposed model achieved 98% overall accuracy on the UNSW-NB15 dataset, outperforming baseline models. The enhanced Gini index feature selection method reduced dimensionality, avoiding

(ELSIVER)				overfitting, and resulted in a lower false alarm rate of only 2% on testing instances.
Muhammad Aamir, Mustafa Ali Zaidi (2019), 18, 761-785 **International Journal of Information Security (SPRINGER)**	DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation	Feature Engineering (backward elimination, chi2, information gain scores), Machine Learning (K-nearest neighbors, Support Vector Machine, Random Forest)	DDoS datasets	Significant feature reduction (approximately 68%) possible with minimal performance hit (about 0.03% on accuracy). K-nearest neighbors algorithm performs best, followed by Support Vector Machine, with Random Forest better on low-dimensional datasets.
Deepak Kumar, R.K. Pateriya, Rajeev Kumar Gupta, Vasudev Dehalwar, Ashutosh Sharma (2023) **ELSEVIER**	DDoS Detection using Deep Learning	Long Short-Term Memory (LSTM), Feature Selection and Extraction	CICDDoS2019	The LSTM-based model achieves up to 98% accuracy in detecting DDoS threats, outperforming traditional ML methods on the CICDDoS2019 dataset.
Muhammad Saibtain Raza, Mohammad Nowsin Amin Sheikh, I-Shyan Hwang, Mohammad Syuhaimi Ab-Rahman (2024) **Telecom**	Feature-Selection-Based DDoS Attack Detection Using AI Algorithms	NGBoost, Convolutional Neural Network (CNN), Stochastic Gradient Descent (SGD), Decision Tree, Random Forest	CICDDoS2019	Natural Gradient Boosting and Convolutional Neural Networks show promise with tabular data categorization.
Sanjalawe, Yousef & Althobaiti, Turke. (2023). **Computers, Materials & Continua**. 75. 3571-3588. 10.32604/cmc.2023.037386.	DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning.	Hybrid deep learning model combining Convolutional Neural Network (CNN) with Long-Short-Term Memory (LSTM). Ensemble feature selection using Particle Swarm Optimizer (PSO), Grey Wolf Optimizer (GWO), Krill Herd (KH), and Whale Optimization Algorithm (WOA).	CICIDS 2017	Achieved detection rates of 97.9%, 98.3%, 97.9%, and 98.1% for various metrics. Outperforms existing IDSs in detecting DDoS attacks in cloud environments, ensuring high security, efficiency, and automatic detection capabilities.
Zakieh Sharifian, Behrang Barekatain, Alfonso Ariza Quintana, Zahra Beheshti, Faramarz Safi-Esfahani. (2023). **Expert Systems with Applications**. Volume 228. 120404. ISSN 0957-4174.	Sin-Cos-bIAVOA: A new feature selection method based on improved African vulture optimization algorithm and a novel transfer function to DDoS attack detection.	Binary Improved African Vulture Optimization Algorithm (Sin-Cos-bIAVOA) enhanced with Sin-Cos compound transfer function for feature selection. Gravitational Fixed Radius Nearest Neighbor (GFRNN) used as classifier.	CIC-DDOS2019, NSL-KDD	Achieved minimum feature selection rate (0.0184) with high average accuracy (99.9979%), precision (99.9979%), recall (100.00%), and F-measure (99.9989%) compared to competitors in CIC-DDOS2019 dataset. Ranked first in Friedman test based on fitness functions.

The reviewed literature highlights significant advancements in DDoS detection using machine learning and deep learning techniques with enhanced feature engineering, achieving higher accuracy rates with models like Random Forest, SVM, and LSTM on datasets such as CICDDoS2019, NSL-KDD, UNSW-NB15. However, these models often suffer from high computational complexity, making them unsuitable for real-time applications. Issues such as class imbalance, high time complexity, and limited dataset diversity also persist. To address these gaps, a Complexity-Aware Intelligent IDS is proposed, aiming to balance detection accuracy with reduced computational overhead. This system would leverage machine and deep learning models and optimized feature selection techniques to ensure efficient DDoS detection suitable for dynamic environments.

3. Definition of the problem

To devise a complexity aware intelligent intrusion detection mechanism specifically for detecting DDoS attacks, with a focus on single-vector and multi-vector DDoS flooding attacks, as well as diverse DDoS attack types.

4. Objectives and scope of research work

The goals are formed after the study of literature to overcome the limitations of the existing architecture. The foremost objective of the research work is to devise a complexity aware intelligent intrusion detection mechanism for detecting DDoS attacks with enhanced feature engineering. Based on the above discussions, the secondary objectives of the thesis are formulated as follows.

(i) To accurately detect single-vector DDoS flooding attacks with improved detection accuracy and minimized computational time.

(ii) To detect multi-vector DDoS flooding attacks with high Performance and low false alarm rate.

(iii) To accurately detect multiple DDOS attacks with high Performance, low false alarm, and scalability.

(iv) To accurately detect DDOS attacks with reduction in computational complexity and high performance across diverse datasets.

5. Research Methodology

The primary objective of this thesis is to develop a complexity aware intelligent intrusion detection system (IDS) with enhanced feature engineering to effectively detect Distributed Denial of Service (DDoS) attacks, which is of paramount importance. A methodological framework is developed with data preprocessing techniques, feature selection techniques, and machine learning and Deep Learning models for detecting Single DDoS Flooding attacks, multiple DDoS Flooding attacks, and multiple DDoS attacks. The proposed research design encompasses data collection, various algorithms and techniques for Feature Selection, and thorough evaluation to achieve the objective of accurately detecting DDoS attacks. Additionally, various computational intelligence techniques are employed to optimize the feature extraction and selection process, complemented by the application of Machine and Deep Learning algorithms. Through rigorous evaluation of the IDS's performance under diverse conditions, reliability and efficacy in mitigating DDoS threats will be ensured. The methodology proposed is shown in Figure 1.

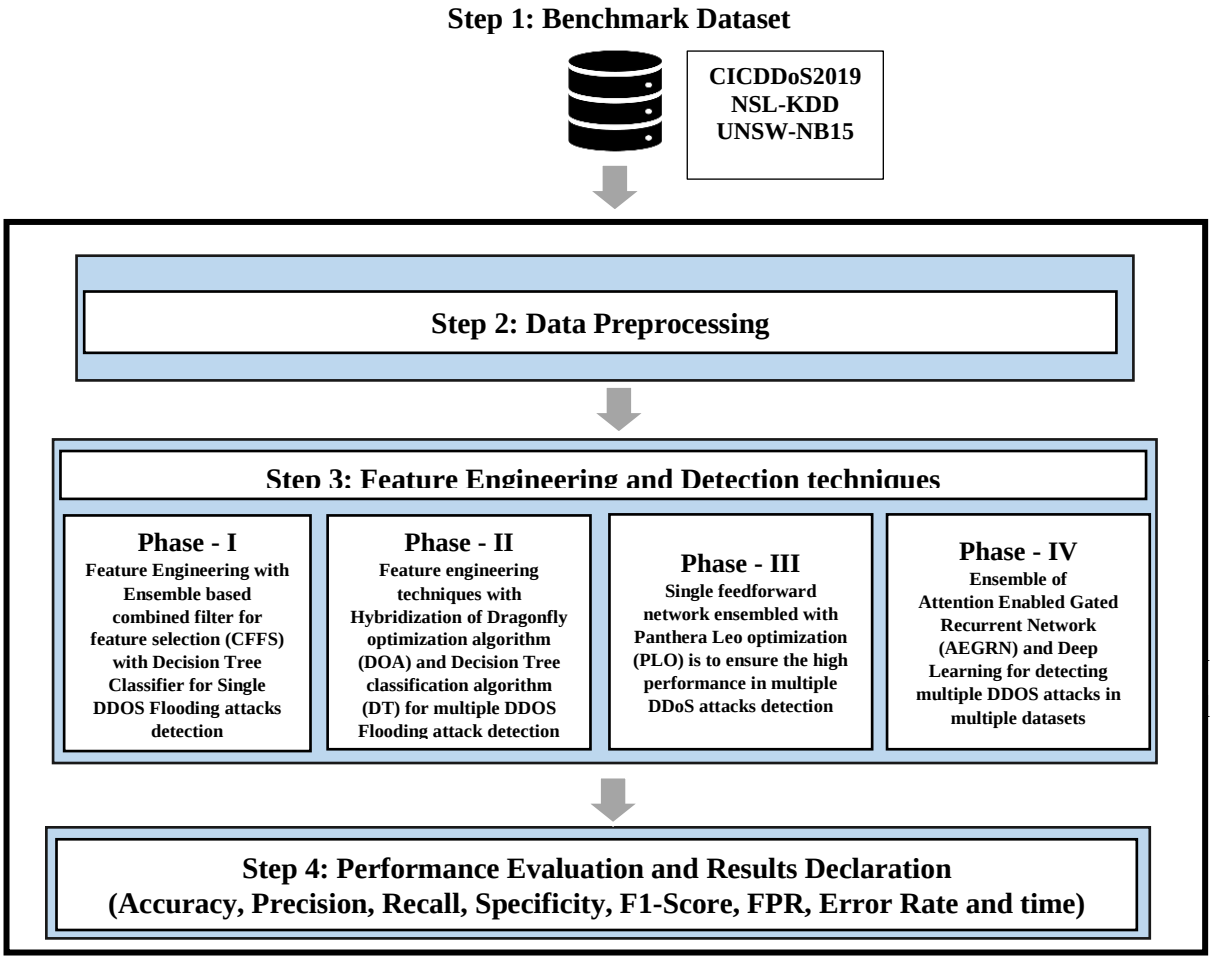
Step 1: Benchmark Dataset
CICDDoS2019
NSL-KDD
UNSW-NB15
Step 2: Data Preprocessing
Step 3: Feature Engineering and Detection techniques
Phase - I
Feature Engineering with Ensemble based combined filter for feature selection (CFFS) with Decision Tree Classifier for Single DDOS Flooding attacks detection
Phase - II
Feature engineering techniques with Hybridization of Dragonfly optimization algorithm (DOA) and Decision Tree classification algorithm (DT) for multiple DDOS Flooding attack detection
Phase - III
Single feedforward network ensembled with Panthera Leo optimization (PLO) is to ensure the high performance in multiple DDoS attacks detection
Phase - IV
Ensemble of Attention Enabled Gated Recurrent Network (AEGRN) and Deep Learning for detecting multiple DDOS attacks in multiple datasets
Step 4: Performance Evaluation and Results Declaration
(Accuracy, Precision, Recall, Specificity, F1-Score, FPR, Error Rate and time)

Figure 1: Overview of the Proposed Research Methodology

The overall research design follows this four-step methodology to efficiently detect DDoS attacks. The first step is to identify the appropriate dataset to validate the proposed model. In the second step, preprocessing of the data is performed, which includes eliminating missing values, handling null values, and normalizing the data. In step three, the proposed feature engineering and detection techniques are applied to detect the DDoS attacks, which enhances the accuracy and robustness of the detection process. Step four involves evaluating the performance using various metrics, validating the results, and comparing them with existing models. The results will demonstrate that the proposed model performs well in detecting DDoS attacks in the digital landscape, providing improved detection accuracy and reliability.

6. Research Contributions

The overall research design and contributions of the thesis is represented in Figure 2.

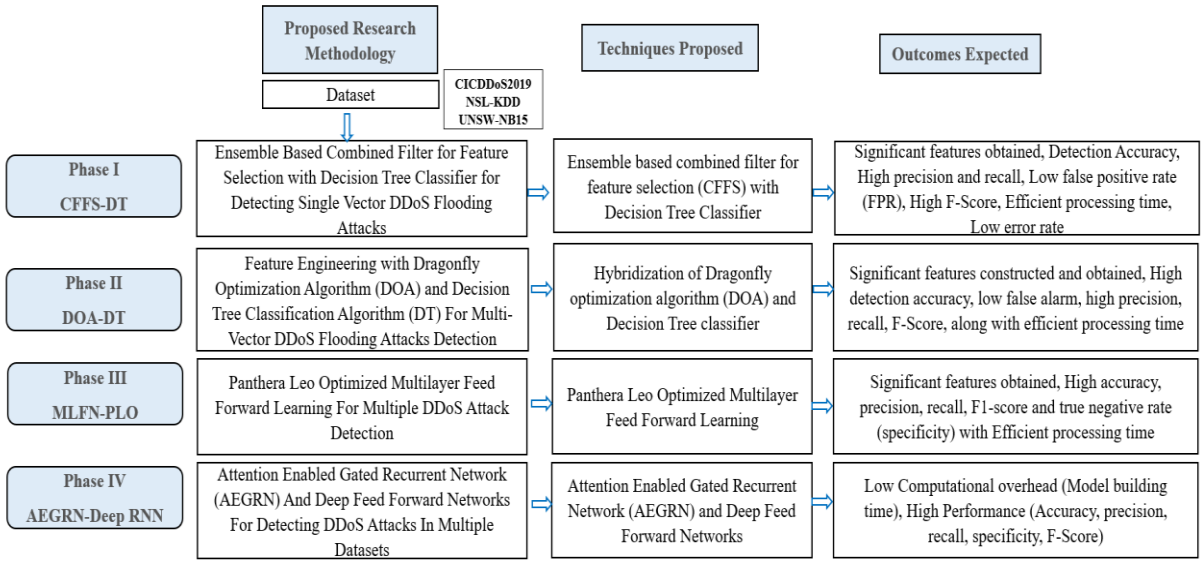
Proposed Research Methodology
Techniques Proposed
Outcomes Expected
Dataset
CICDDoS2019
NSL-KDD
UNSW-NB15
Phase I
CFFS-DT
Ensemble Based Combined Filter for Feature Selection with Decision Tree Classifier for Detecting Single Vector DDoS Flooding Attacks
Ensemble based combined filter for feature selection (CFFS) with Decision Tree Classifier
Significant features obtained, Detection Accuracy, High precision and recall, Low false positive rate (FPR), High F-Score, Efficient processing time, Low error rate
Phase II
DOA-DT
Feature Engineering with Dragonfly Optimization Algorithm (DOA) and Decision Tree Classification Algorithm (DT) For Multi-Vector DDoS Flooding Attacks Detection
Hybridization of Dragonfly optimization algorithm (DOA) and Decision Tree classifier
Significant features constructed and obtained, High detection accuracy, low false alarm, high precision, recall, F-Score, along with efficient processing time
Phase III
MLFN-PLO
Panthera Leo Optimized Multilayer Feed Forward Learning For Multiple DDoS Attack Detection
Panthera Leo Optimized Multilayer Feed Forward Learning
Significant features obtained, High accuracy, precision, recall, F1-score and true negative rate (specificity) with Efficient processing time
Phase IV
AEGRN-Deep RNN
Attention Enabled Gated Recurrent Network (AEGRN) And Deep Feed Forward Networks For Detecting DDoS Attacks In Multiple Datasets
Attention Enabled Gated Recurrent Network (AEGRN) and Deep Feed Forward Networks
Low Computational overhead (Model building time), High Performance (Accuracy, precision, recall, specificity, F-Score)

Figure 2. Research contributions and Design

7. Experimental Results and Discussion

This section presents the key findings of the research and provides an in-depth analysis of their implications. The results obtained from the proposed complexity aware enhanced feature engineering methods for intelligent DDoS intrusion detection demonstrate significant improvements in detection accuracy, efficiency, and robustness across various attack scenarios. By implementing and testing the four contributions—detecting single and multiple DDoS flooding attacks using ensemble-based feature selection, Dragonfly

Optimization, Panthera Leo Optimized Multilayer Feed Forward Learning, and Attention Enabled Gated Recurrent Network (AEGRN) with deep learning—each approach was evaluated against relevant datasets to assess performance metrics such as detection rate, false positive rate, and computational overhead. The discussion will interpret these results, highlighting the strengths and potential areas for further refinement in the proposed models.

Phase I - Ensemble Based Combined Filter for Feature Selection (CFFS) With Decision Tree (DT) Classifier for Single DDoS Flooding Attacks Detection

This phase proposes Combined filter for feature selection (CFFS) method, which combines the output of the information gain (IG), gain ratio, chi-squared, and ReliefF to pick the essential features. Decision Tree C4.5 (DT) and Support Vector Machines (SVM) are chosen for evaluation due to their widespread use, versatility, and effectiveness in various classification tasks. Both algorithms have proven track records in machine learning applications, making them suitable for evaluating performance against Single DDoS Flooding attacks such as (UDP Flood, ICMP Flood, DNS Flood, SYN Flood, ACK Flood).

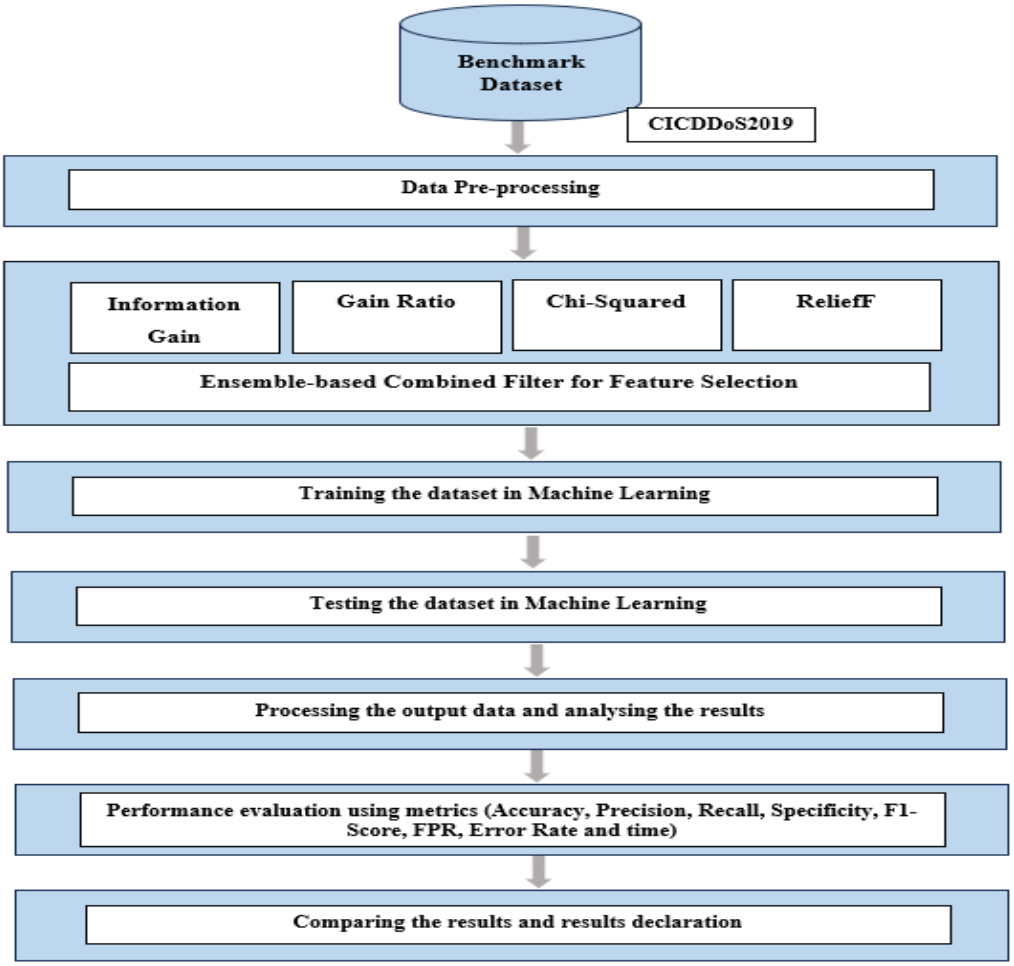
Benchmark Dataset
CICDDoS2019
Data Pre-processing
Information Gain
Gain Ratio
Chi-Squared
ReliefF
Ensemble-based Combined Filter for Feature Selection
Training the dataset in Machine Learning
Testing the dataset in Machine Learning
Processing the output data and analysing the results
Performance evaluation using metrics (Accuracy, Precision, Recall, Specificity, F1-Score, FPR, Error Rate and time)
Comparing the results and results declaration

Figure 3. Proposed Model in Phase I

The proposed methodology is assessed using the CICDDOS2019 intrusion detection benchmark dataset with 80 characteristics. Figure 3 shows the proposed model in Phase I. The suggested ensemble-based feature selection method is put up against several filtering techniques using machine learning algorithms such as Decision Tree C 4.5 and SVM. The comparison of the various metrics of the different classification model is shown in Figure 4 and the comparison of the accuracy rate, precision, recall, FPR, F-Score and time attained by suggested models is shown in Table 2 that are trained using the CICDDoS2019 dataset. The collected findings demonstrate that the suggested technique outperforms the other method of individual filter-based feature selection methods.

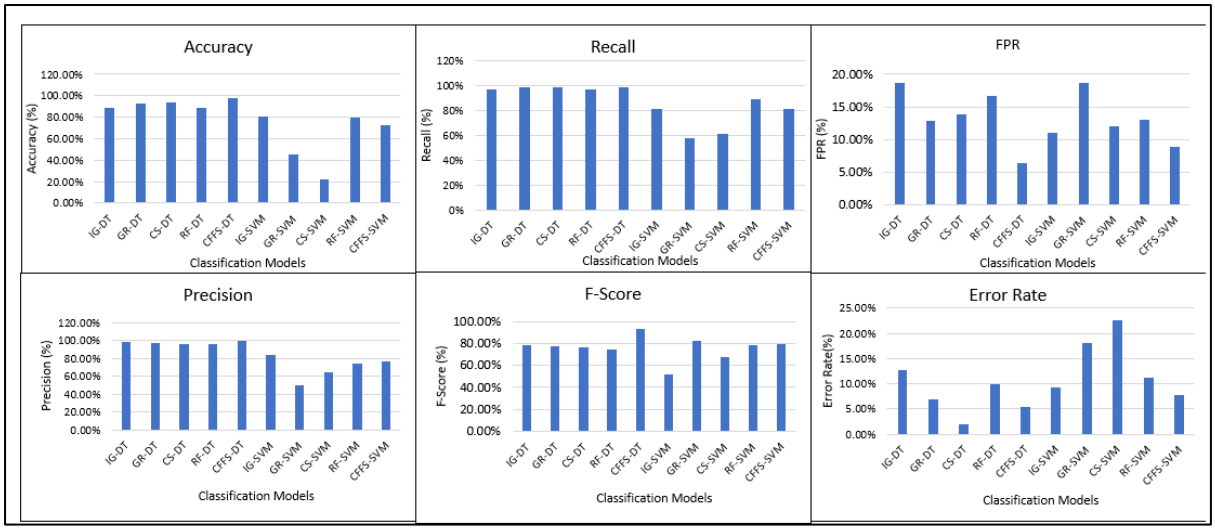

Figure 4. Performance metrics of the proposed model in Phase I

Table 2. Performance Measures for Phase I

Approaches	Accuracy (%)	Precision (%)	Recall (%)	FPR (%)	F-Score (%)	Time (S)	Error Rate (%)
IG-DT	88.64	98.25	97	18.71	78.76	5.37	12.61
GR-DT	92.23	97.51	98.50	12.80	77.45	2.64	6.96
CS-DT	93.26	96.62	98.70	13.79	76.16	1.87	5.01
RF-DT	89.16	96.01	97.50	16.74	74.80	1.64	10.00
CFFS-DT	**97.69**	**99.13**	**98.50**	**6.32**	**92.90**	**1.2**	**5.40**
IG-SVM	80.63	83.50	81.25	10.94	51.34	4.92	9.36
GR-SVM	44.88	50.46	58.20	18.62	82.43	5.24	18.12
CS-SVM	22.47	64.52	61.20	12.04	67.33	3.18	22.52
RF-SVM	79.86	74.70	89.25	13.00	78.67	7.66	11.14
CFFS-SVM	72.16	76.59	81.75	8.81	79.82	1.7	7.84

The suggested model in Phase I is performing well for Single DDoS Flooding attack, when evaluating the proposed approach against Multiple DDoS Flooding attacks, its performance decreases. Therefore, it becomes essential to introduce a more intelligent approach to counteract Multiple Flooding attacks.

Phase II - Feature Engineering Techniques with Hybridization of Dragonfly Optimization Algorithm (DOA) And Decision Tree Classification Algorithm (DT) For Multiple DDoS Flooding Attacks Detection

Based on the limitations discussed in the first contribution, phase II two proposes a Strategic-Framework with computational intelligence for feature selection and machine learning for classification. The proposed framework will improve the accuracy and reduce computational delay during the multiple DDoS attack detection. Hybridizing the Dragonfly Optimization Algorithm (DOA) with the Decision Tree C 4.5 Classification Algorithm (DT), this framework aims to optimize feature engineering processes, resulting in more precise and efficient identification of relevant features.

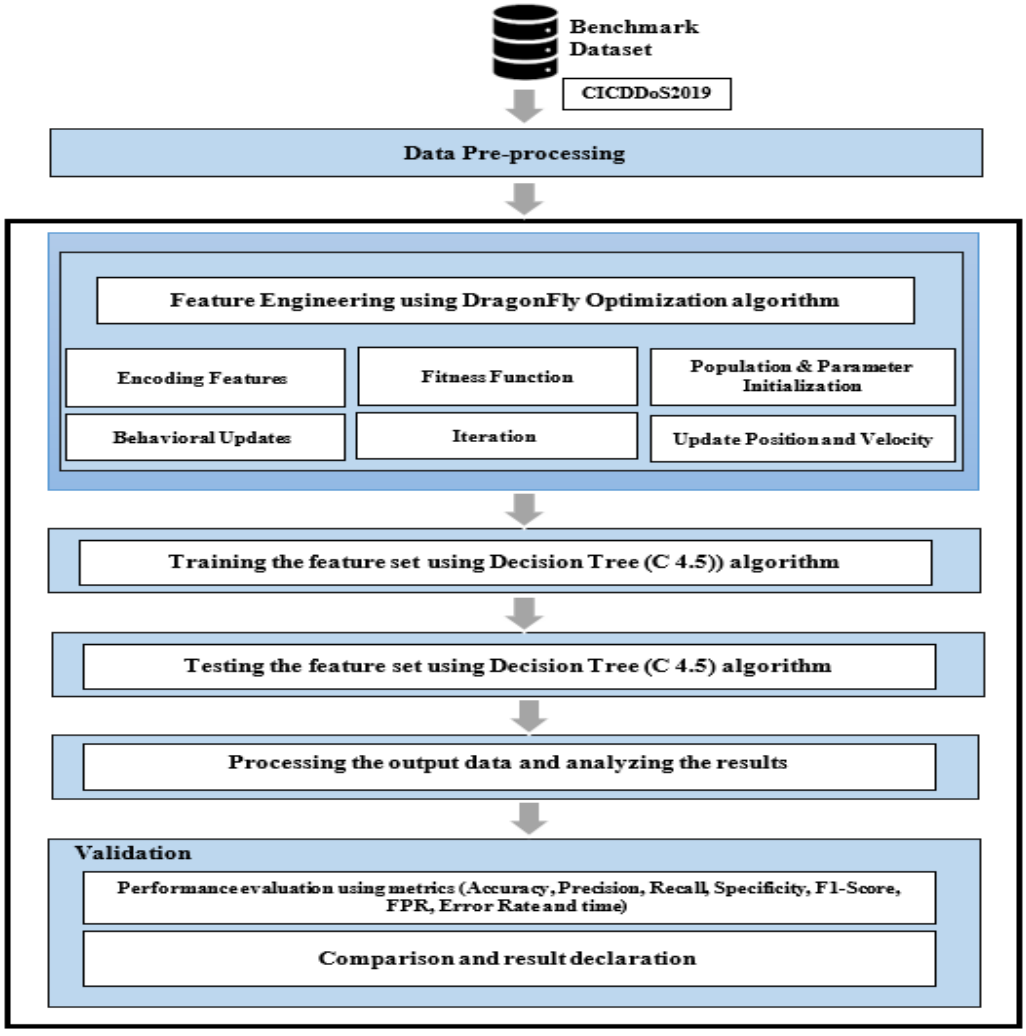
Benchmark Dataset
CICDDoS2019
Data Pre-processing
Feature Engineering using DragonFly Optimization algorithm
Encoding Features
Fitness Function
Population & Parameter Initialization
Behavioral Updates
Iteration
Update Position and Velocity
Training the feature set using Decision Tree (C 4.5)) algorithm
Testing the feature set using Decision Tree (C 4.5) algorithm
Processing the output data and analyzing the results
Validation
Performance evaluation using metrics (Accuracy, Precision, Recall, Specificity, F1-Score, FPR, Error Rate and time)
Comparison and result declaration

Figure 5. Proposed Model in Phase II

The experiments are conducted using the CICDDoS2019 dataset. The results are discussed in detail to provide insights into the performance of the hybrid approach and its

potential implications for cybersecurity applications. The proposed model for Phase II is shown in Figure 5. The suggested framework with Dragonfly optimization for detecting multiple DDoS attack detection is validated with various combinations using machine learning algorithms. Multiple DDoS Flooding attacks such as UDP Flood + ICMP Flood, DNS + NTP, UDP Flood + HTTP Get Flood, TCP Flood + HTTP POST Flood are considered. A comparison bar graph for the various metrics attained by suggested framework that are trained using the CICDDoS2019 dataset is shown in Figure 5. The collected findings demonstrate that the suggested framework performs well with the combination of Dragonfly Optimization Algorithm with Decision Tree C 4.5 classification algorithm in terms of accuracy, precision, recall, and F-measure. The comparison of the various metrics of the different classification model is shown in Figure 6. Table 3 represents the classification metric values for the proposed strategic framework model with different alternatives.

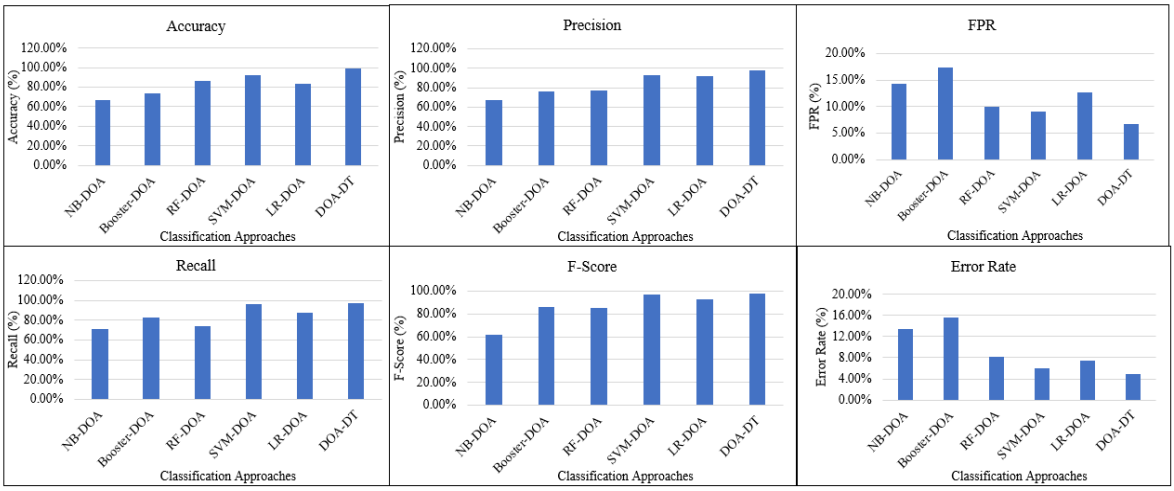

Figure 6. Performance metrics of the proposed Strategic level framework

Table 3: Proposed framework model's execution and calculations

Approaches	Accuracy (%)	Precision (%)	Recall (%)	F-Score (%)	Time (s)	FPR (%)	Error Rate (%)
NB-DOA	67.00	67.00	71.00	62.00	1.24	14.22	13.48
Booster-DOA	74.00	76.00	83.00	86.00	0.78	17.28	15.62
RF-DOA	86.00	77.00	74.00	85.00	1.85	10.06	8.09
SVM-DOA	92.00	93.00	96.00	97.00	0.93	9.00	6.01
LR-DOA	83.00	92.00	88.00	93.00	0.96	12.59	7.39
DOA-DT	**98.89**	**98.00**	**97.00**	**98.00**	**0.69**	**6.71**	**4.99**

When comparing the Dragonfly Optimization Algorithm with a Decision Tree (DOA-DT) to other combinations, the DOA-DT approach yields the highest performance metrics:

Precision (98.00%), Recall (97.00%), F-Score (98.00%), Accuracy (98.89%), and execution time (0.69). This highlights the efficacy of the DOA-DT combination over other methods. The experimental results demonstrated that proposed approach detects multiple flooding attacks with improved accuracy and comparatively less detection time. A 10-fold cross-validation is performed to ensure the robustness and reliability of the results, providing a comprehensive assessment of the model's performance, and reducing the risk of overfitting. However, when multiple DDoS attack types are introduced, it becomes evident that more advanced optimization techniques are required to further enhance detection accuracy, reduce computational time, and minimize system complexity.

Phase III - Panthera Leo Optimized Multilayer Feed Forward Learning for Multi Vector DDoS Attack Detection

Based on the limitations discussed in the previous contribution, this phase suggests employing a Multi Feedforward Layer Network (MLFFN) enhanced with Panthera Leo Optimization (PLO) methods for both feature selection and classification. By adopting this proposed framework, enhancements in accuracy and reductions in computational latency, among other benefits, can be expected in the context of detecting multiple DDoS attacks such as UDP Flood, TCP SYN Flood, HTTP GET Flood, DNS Amplification, NTP Amplification, UDP + HTTP GET Flood, TCP SYN + HTTP POST Flood.

The proposed model for Phase III is shown in Figure 7. The experimental results obtained by applying the Panthera Leo Optimization (PLO) Algorithm in conjunction with the Multi-Layer Feed-Forward Network (MLFFN) for detecting DDoS attacks is presented and analysed. The experiments are conducted using the CICDDoS2019 dataset. The objective is to assess the effectiveness of this hybrid approach in feature selection enhancement and detection accuracy improvement. The results presented is to gain insights into the performance of the PLO-MLFFN framework and its potential implications for cybersecurity applications. The performance measures accuracy, precision, recall, specificity, FPR, Error Rate, F1-Score and time are used to assess the proposed model and are calculated using the mathematical expressions.

Confusion matrix for the proposed model is shown in Figure 8 shows the performance of a proposed algorithm in correctly classifying different types of network attacks, with high percentages along the diagonal indicating accurate predictions. Furthermore, the proposed design is compared to other models in use by predicting various display measurements.

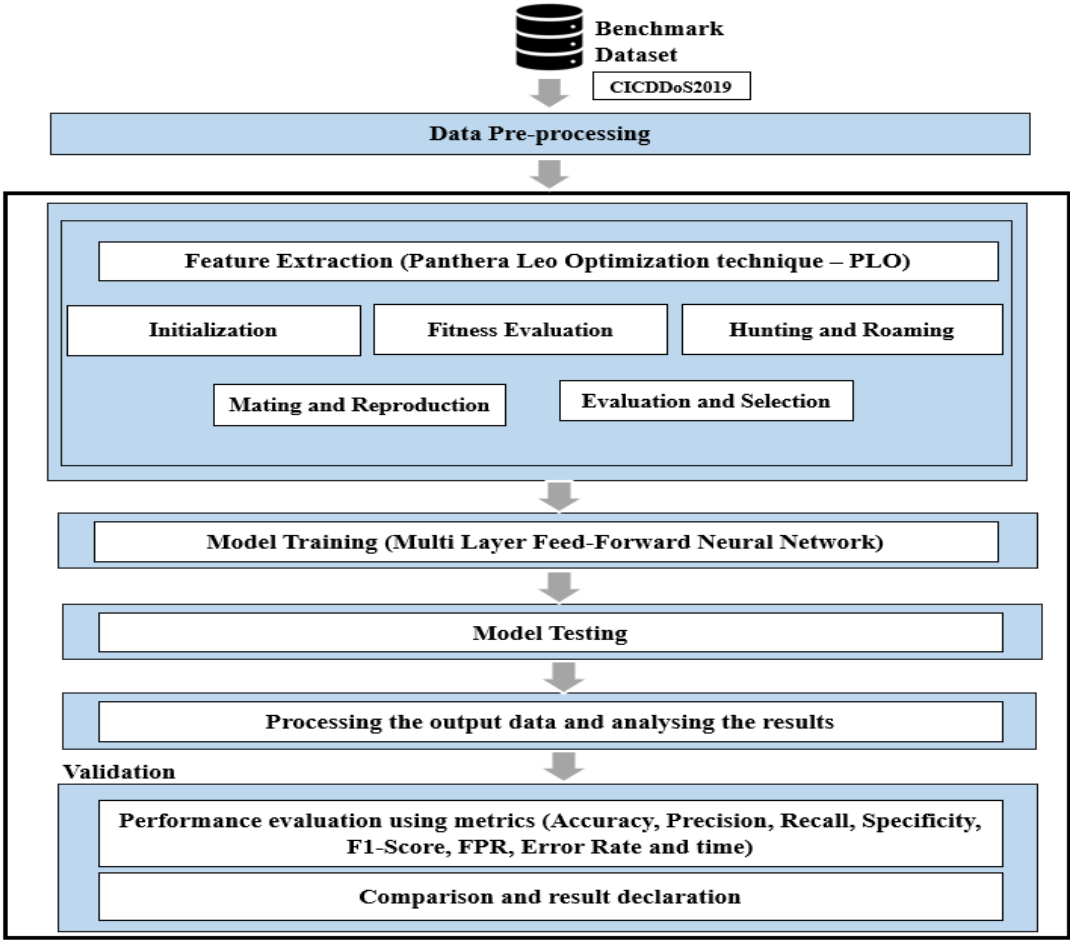
Benchmark Dataset
CICDDoS2019
Data Pre-processing
Feature Extraction (Panthera Leo Optimization technique – PLO)
Initialization
Fitness Evaluation
Hunting and Roaming
Mating and Reproduction
Evaluation and Selection
Model Training (Multi Layer Feed-Forward Neural Network)
Model Testing
Processing the output data and analysing the results
Validation
Performance evaluation using metrics (Accuracy, Precision, Recall, Specificity, F1-Score, FPR, Error Rate and time)
Comparison and result declaration

Figure 7. Proposed model in Phase III

Confusion matrix for the Proposed algorithm

Actual Values \ Predicted Values	UDP Flood	TCP SYN Flood	HTTP GET Flood	DNS Amplification Attack	NTP Amplification Attack	UDP Flood + HTTP GET Flood	TCP SYN Flood + HTTP POST Flood
UDP Flood	96.80%	0.50%	0.50%	0.50%	0.50%	0.60%	0.60%
TCP SYN Flood	0.50%	96.70%	0.50%	0.50%	0.60%	0.60%	0.60%
HTTP GET Flood	0.50%	0.60%	96.75%	0.50%	0.60%	0.60%	0.60%
DNS Amplification Attack	0.50%	0.50%	0.50%	96.85%	0.60%	0.50%	0.50%
NTP Amplification Attack	0.50%	0.50%	0.60%	0.50%	96.78%	0.60%	0.50%
UDP Flood + HTTP GET Flood	0.60%	0.60%	0.50%	0.50%	0.60%	96.80%	0.50%
TCP SYN Flood + HTTP POST Flood	0.50%	0.60%	0.50%	0.50%	0.50%	0.60%	96.80%

Figure 8. Confusion Matrix of the proposed model in Phase III

This work compared the suggested IDS to other state-of-the-art existing IDS at various training dataset proportions to demonstrate its superiority. The results are shown for various ratios of datasets in Figure 9.

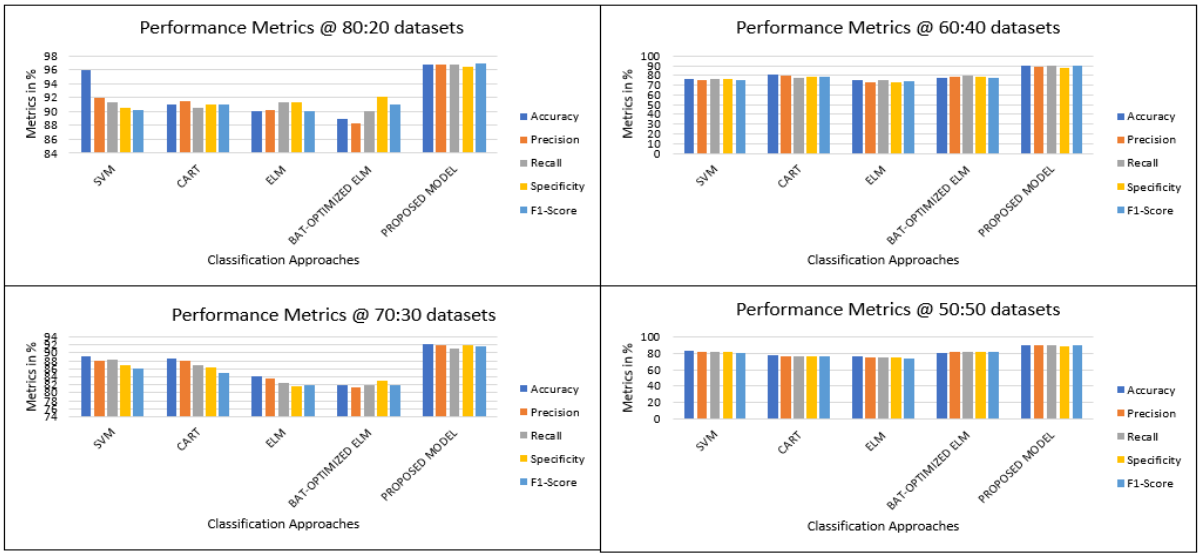

Figure 9. Comparative Analysis of the Different IDS at the different ratio of datasets

Multiple DDoS attack types show that the proposed model outperforms other approaches in terms of accuracy, precision, recall, specificity, and F1-score, demonstrating consistently noticeable performance across all metrics shown in Figure 10.

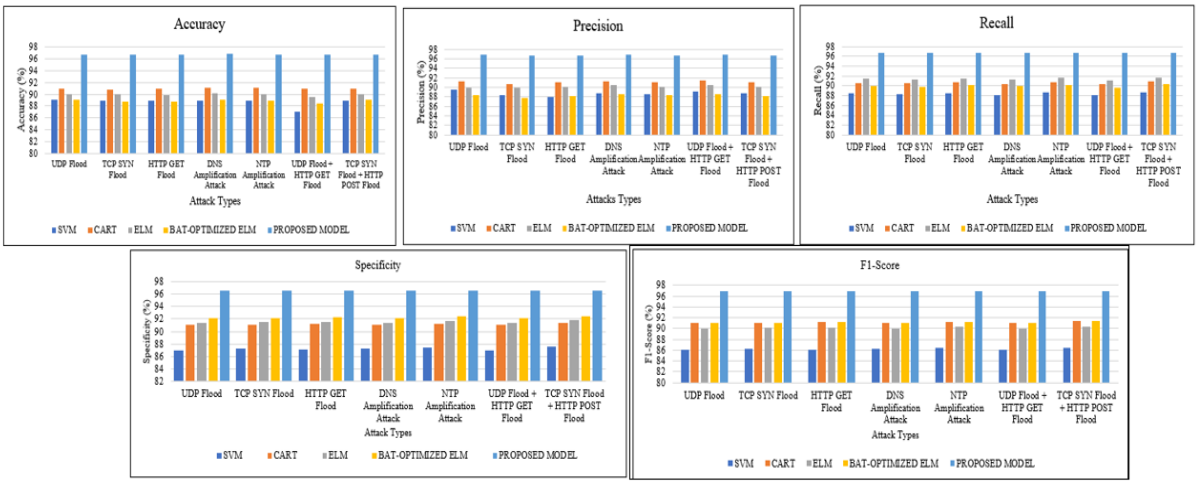

Figure 10. Comparison of the different attack types using the proposed method in phase III

Table 4. Comparative Analysis of the Different IDS in terms of detection time of attacks

Sl.no	Algorithms	Detection time(sec) – per epochs			
		80:20	70:30	60:40	50:50
1	**SVM**	9.4	12.3	13.5	14.3
2	**CART**	10.4	13.0	14.2	15.3
3	**ELM**	11	13.2	14.3	15.3
4	**BAT-ELM**	9.1	9.1	9.0	8.9
5	**PLO-ELM**	**7.6**	**7.6**	**7.5**	**7.5**

Table 4 shows detection time of different IDS. The proposed algorithm's ability to maintain constant detection time during data split testing, even with an increased number of attacks, adds significant value. It demonstrates the algorithm's efficiency and robustness, ensuring consistent performance and reliability across different data distributions. This stability is crucial for guaranteeing prompt and effective response to threats, thereby enhancing the overall security and efficiency of the IDS in dynamic and high-traffic environments.

In Phase III the proposed framework integrates Panthera Leo Optimized Multilayer Feed Forward Learning with improved performance, reduced false alarm and scalability in detecting multiple DDoS attacks. Proposed framework achieves accuracy of 96.8%, precision of 96.75%, recall of 96.73%, specificity of 96.5%, and F1-score of 96.89% across different dataset training and testing ratios. Comparative analysis across various algorithms and datasets consistently showed significant performance of the proposed IDS, even as the number of malicious nodes increased. The PLO-MLFFN algorithm consistently exhibits the lowest detection times across all partition ratios of training and test data (80:20, 70:30, 60:40, and 50:50) compared to other algorithms such as SVM, CART, ELM, and BAT-ELM. This indicates that PLO-MLFFN is the most efficient algorithm with 7.6 secs. The proposed model in Phase III is effective for detecting and dealing with multiple DDoS attacks. However, the model needs further enhancement to handle larger scales and multiple datasets with low computational overhead and high prediction performance.

Phase IV - Attention Enabled Gated Recurrent Network (AEGRN) and Deep Feed Forward Networks for Detecting DDoS Attacks in Multiple Datasets

This phase explores the effectiveness of Attention-Enabled Gated Recurrent Networks (AEGRN) and Deep Feedforward Networks in detecting DDoS attacks across diverse datasets. By combining recurrent neural networks (RNNs) with attention mechanisms and leveraging deep learning capabilities, this research aims to enhance detection accuracy and resilience against DDoS threats. Strengthening feature extraction step is essential for improving the performance and robustness of intrusion detection systems (IDS) in identifying DDoS attacks. Effective feature extraction enhances model accuracy by identifying the most relevant features and reducing noise, which helps in uncovering complex patterns and subtle anomalies indicative of attacks. The proposed model for Phase IV is shown in Figure 11.

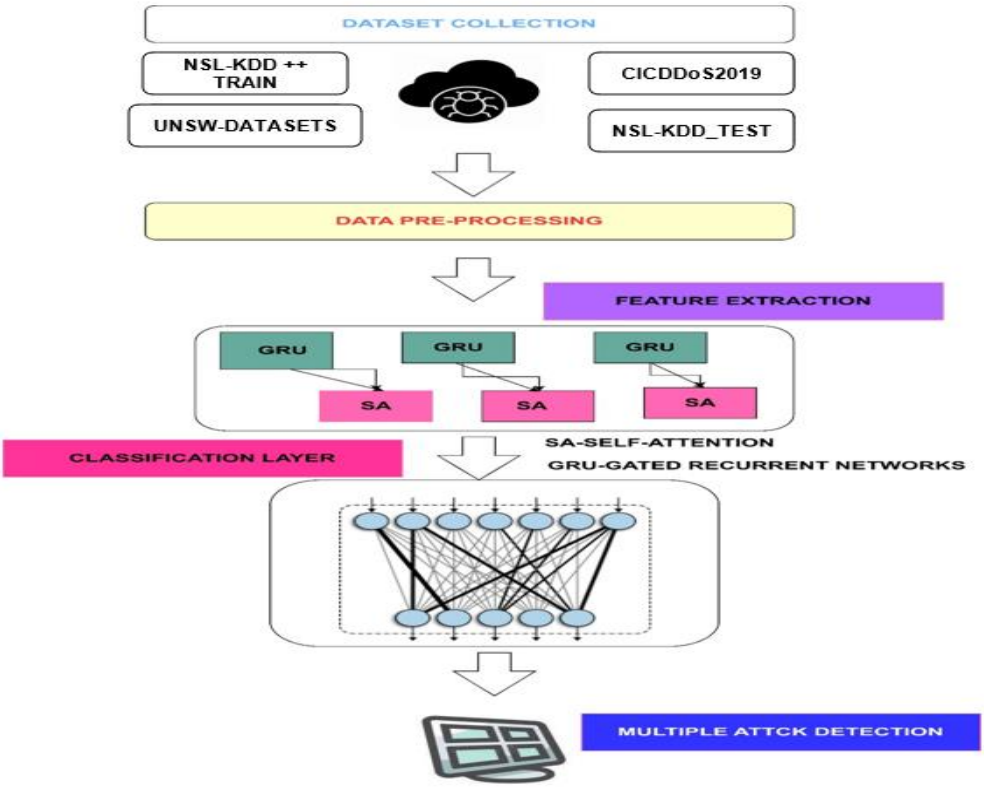

Figure 11. Proposed model in Phase IV

The hybrid suggested network's framework is made up of three sub modules. In the first module, multiple datasets are pre-processed and inputted to the proposed network. The second module consists of the proposed SA-GRU-FF framework in which attention layer is integrated to remove redundant and non-optimal temporal features. These features are then fed into the fully connected deep feed forward networks for classification of the multiple attacks. The experimentation is carried out based on component structures with the same parameters as the proposed framework with different datasets. In detail, the validation of the proposed existing structures includes Long Short-Term Memory**,** Gated Recurrent Units**,** Optimized GRU, and BiGRU**.** The technique is validated, and a comparison study is performed using four different datasets shown in Figure 12.

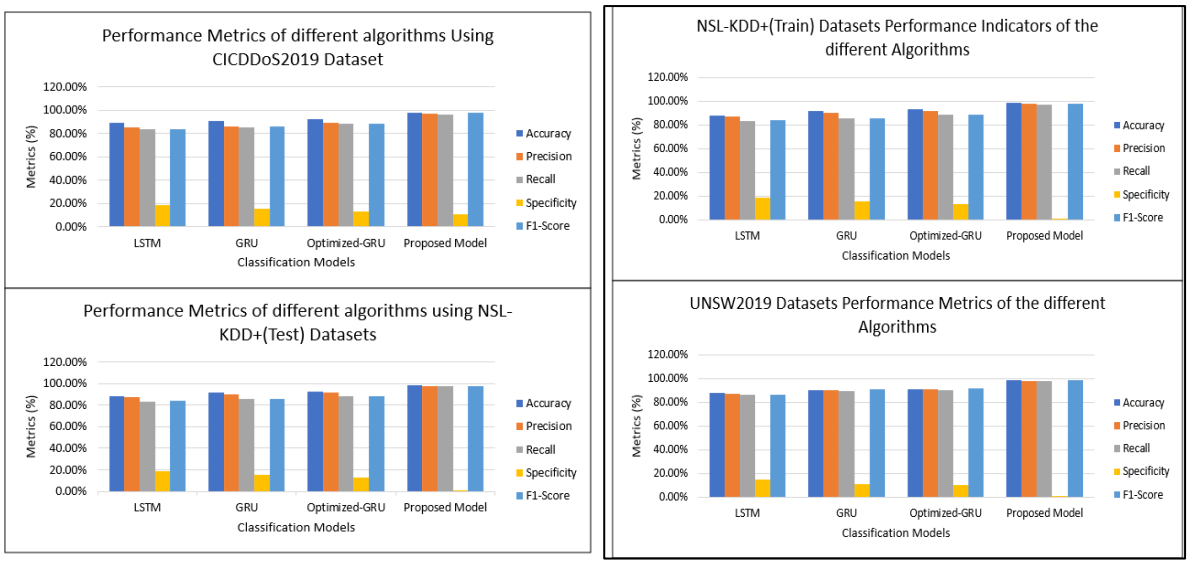

Figure 12. Performance Comparison using various Dataset

The suggested model GRU-SA-FF has demonstrated the best performance in detecting the numerous attacks. The integration of Self-attention maps has provided the best results in contrast to distinct techniques based on deep learning. Table 5 summarizes model building times (MBT in seconds) across different datasets using various classifiers in hold-out evaluation.

Table 5. MBT in support of Different Algorithms using Different Datasets

Datasets	**(MBT)-Secs (per epoch)**			
	LSTM	**GRU**	**Op-LSTM**	**Proposed Model**
CICDDoS2019	34.2	31.2	26.4	**18**
UNSW	31.2	27.6	22.8	**16.8**
NSL-KDD++ Train	34.2	31.2	26.4	**17.4**
NSL-KDD++ Test	30	29.4	27	**17.4**
Average MBT	32.4	29.85	25.65	**17.4**

The analysis of model building times (MBT) for various classifiers demonstrates the importance of efficient training in threat detection systems. The proposed model exhibits an average MBT of 17.4 seconds per epoch across different datasets, significantly outperforming Op-LSTM (32.4s), GRU (29.85s), and LSTM (25.65s). This efficiency is crucial for designing defense systems against multiple attacks, achieving a favorable balance between computational complexity and classifier performance. The model's high accuracy (98.00% to 98.80%), precision (97.00% to 98.00%), recall (96.60% to 97.40%), and F1-Score (97.50% to 98.30%) across various datasets highlight its robustness and reliability in identifying normal

and attack traffic with minimal errors. Despite the low specificity values (0.10% to 1.10%), the model prioritizes detecting true positives over avoiding false positives, ensuring comprehensive threat detection. This approach, combined with the low MBT, validates the model's scalability and efficiency, making it ideal for deployment in large, diverse environments where high performance and low computational costs are essential.

Phase V - Statistical validation and proposed model comparison in DDoS Attack detection

In Phase V, the statistical validation and comparison of proposed models for DDoS attack detection is detailed. Given the increasing sophistication and frequency of DDoS attacks, robust detection mechanisms are critical. This chapter employs ANOVA, p-Test, and F-Test to validate and compare various machine learning (ML) and deep learning (DL) models. ANOVA analysis highlights the importance of "between groups" and "within groups" variances, determining if differences in model accuracy are statistically significant. Four innovative models are proposed: Combined Filter for Feature Selection (CFFS) with Decision Tree C 4.5 (DT) classifier, Hybrid Feature Engineering with Dragonfly Optimization Algorithm (DOA) and DT, Panthera Leo Optimized Multilayer Feed Forward Network, and an ensemble model of Attention Enabled Gated Recurrent Network (AEGRN) and Deep Feed Forward Networks. Each model demonstrated significant improvements in accuracy, efficiency, and execution time over traditional methods. The ANOVA results consistently showed high F-values and low p-values, confirming the statistical significance of the performance differences.

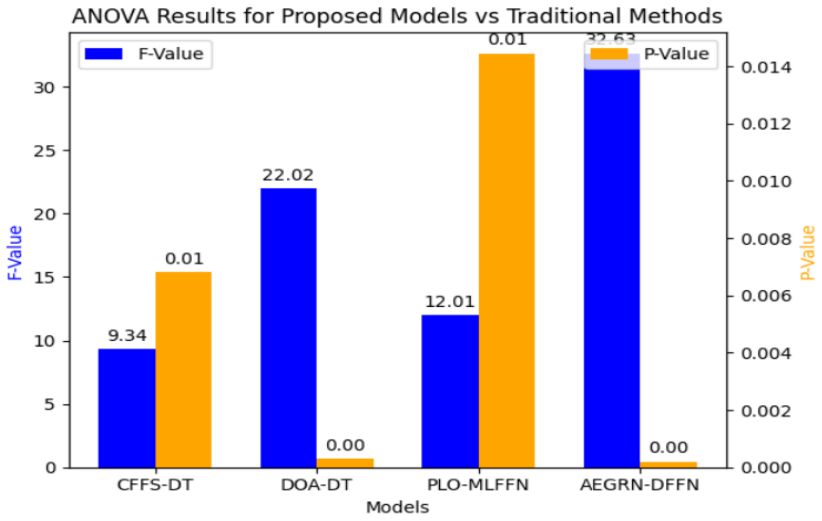

Figure 13. ANOVA results comparison for the proposed models

The ANOVA test is performed to compare the efficacy of four distinct statistical models: CFFS-DT, DOA-DT, PLO-MLFFN, and AEGRN-DFFN. The results are visually

represented in a bar chart in Figure 13, indicating the F and p values for each model. The AEGRN-DFFN model exhibited the highest F value of approximately 32.63, suggesting a significant variance between groups compared to within groups, while maintaining a low p value of around 0.0002, which is indicative of strong evidence against the null hypothesis. The high statistical significance (low p-value) and strong F-value provide confidence that the model's performance metrics are reliable and not due to random variation, making the model a robust and reliable tool for detecting intrusions. These advancements contribute to the development of intelligent intrusion detection systems capable of safeguarding digital infrastructures against evolving DDoS threats.

8. Summary, Conclusion and Future Scope

In conclusion, this comprehensive research work has successfully addressed critical challenges in detecting Distributed Denial of Service (DDoS) attacks by proposing innovative methodologies that leverage advanced machine learning and deep learning techniques. The proposed ensemble-based feature selection methods, hybridization of optimization algorithms with classification techniques, and integration of attention mechanisms into recurrent neural networks have demonstrated remarkable advancements in accuracy, efficiency, and robustness of DDoS intrusion detection systems. Through rigorous experimentation and evaluation across diverse datasets, the proposed solutions have shown superior performance metrics, including accuracy, precision, recall, and computational efficiency, compared to existing approaches. The consolidation of enhanced feature engineering, optimization algorithms, and deep learning architectures has not only enhanced detection capabilities but also covered the way for more resilient and adaptive defense mechanisms against evolving cyber threats. This research contributes significantly to the field of cybersecurity by providing practical and scalable solutions for safeguarding digital landscapes against sophisticated DDoS attacks.

Future research will prioritize validating the intrusion detection system with real-time datasets to enhance its adaptability to evolving cyber threats. Additionally, exploring the deployment of the model in advanced networks will ensure scalability and effectiveness, addressing the influence of AI in the cyber threat landscape.

10. Publications

Journals

- Kalaivani, M., Padmavathi, G. ‘Panthera Leo Optimized Multilayer Feed Forward Learning-

Based Intrusion Detection Model for Cloud." **SN COMPUT. SCI. 4, 800 (2023).** https://doi.org/10.1007/s42979-023-02225-x, **Springer Nature**

- Kalaivani M and Padmavathi G, "Ensembling of Attention-based Recurrent Units for Detection and Mitigation of Multiple Attacks in Cloud" **International Journal of Advanced Computer Science and Applications(IJACSA)**, **14(10), 2023**. http://dx.doi.org/10.14569/IJACSA.2023.0141010 **Indexed in Scopus**

Conferences

- Kalaivani M, Padmavathi G, "Strategic-level framework with combined feature engineering and optimization Methods for detecting DDoS Flooding attacks in Cloud Environment", **CEMC 2022**, **October 29-30, 2022,** published in the Grenze International Journal of Engineering and Technology (GIJET) as Volume 9 Issue 1 (January 2023 issue), https://thegrenze.com/index.php?display=page&view=journaldetails&id=8 . Indexed in **Scopus**.
- Kalaivani M, Padmavathi G, "Hybrid Ensemble based feature engineering techniques for detecting direct DDOS flooding attack in Cloud", **MLIP-2022**, **November 2022,** published in the **Grenze International Journal of Engineering and Technology (GIJET) as Volume 9 Issue 1 (January 2023 issue)**, https://thegrenze.com/index.php?display=page&view=journaldetails&id=8 . Indexed in **Scopus**

11. Significant References

[1] Aswani Devi Aguru, Suresh Babu Erukala. *A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning*, *ELSEVIER*, 2024.

[2] Devrim Akgun, Selman Hizal, Unal Cavusoglu. *A new DDoS attacks intrusion detection model based on deep learning for cybersecurity*, *ELSEVIER*, 2022.

[3] Mohamed Aly Bouke, Azizol Abdullah, Sameer Hamoud ALshatebi, Mohd Taufik Abdullah, Hayate El Atigh. *An intelligent DDoS attack detection tree-based model using Gini index feature selection method Microprocessors and Microsystems (ELSEVIER)*, 2023.

[4] Muhammad Aamir, Mustafa Ali Zaidi. *DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation International Journal of Information Security (SPRINGER)*, 2019, Vol. 18, PP 761-785

[5] Mohammad Najafimehr, Sajjad Zarifzadeh, Seyedakbar Mostafavi. *DDoS attacks and machine-learning-based detection methods: A survey and taxonomy Engineering Reports*, 2023.

[6] Deepak Kumar, R.K. Pateriya, Rajeev Kumar Gupta, Vasudev Dehalwar, Ashutosh Sharma. *DDoS Detection using Deep Learning*, *ELSEVIER*, 2023.

[7] Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis, Helge Janicke *Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study Journal of Information Security and Applications (ELSEVIER)*, 2020, Issue 50

[8] Rifat Al Mamun Rudro, Md. Faruk Abdullah Al Sohan, Syma Kamal Chaity, Rubina Islam Reya. *Enhancing DDoS Attack Detection Using Machine Learning: A Framework with Feature Selection and Comparative Analysis of Algorithms Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 2023

[9] Muhammad Saibtain Raza, Mohammad Nowsin Amin Sheikh, I-Shyan Hwang, Mohammad Syuhaimi Ab-Rahman. *Feature-Selection-Based DDoS Attack Detection Using AI Algorithms Telecom* 2024

[10] Sanjalawe, Yousef & Althobaiti, Turke. *DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning Computers, Materials & Continua* 2023, Vol 75, PP 3571-3588

[11] Zakieh Sharifian, Behrang Barekatain, Alfonso Ariza Quintana, Zahra Beheshti, Faramarz Safi-Esfahani. *Sin-Cos-bIAVOA: A new feature selection method based on improved African vulture optimization algorithm and a novel transfer function to DDoS attack detection Expert Systems with Applications*, 2023, Vol 228, PP 12040

[12] Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani, "*Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy*", IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India, 2019.

[13] M. M. Mafarja, D. Eleyan, I. Jaber, A. Hammouri and S. Mirjalili, "Binary Dragonfly Algorithm for Feature Selection," 2017 International Conference on New Trends in Computing Sciences (ICTCS), 2017, pp. 12-17, doi: 10.1109/ICTCS.2017.43.

[14] Sayed, G.I., Tharwat, A. & Hassanien, A.E. Chaotic dragonfly algorithm: an improved metaheuristic algorithm for feature selection. Appl Intell 49, 188–205 (2019).